REMARKS

Claims 1-38 and 41-61 are pending in the application, and claims 1-26, 28-38 and 41-61 stand rejected.

Rejection under 35 U.S.C §102

Claims 1, 2, 10-32, 38 and 41-61 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Pat. No. 6,694,436 to Audebert. In particular, with regards to claims 1 and 48, the Examiner finds that Audebert discloses all claimed limitations. Applicants have reviewed this new reference with care and are compelled to respectfully disagree with the Examiner's interpretation and characterization of this document.

Audebert is directed to a computer system that includes a transaction terminal (1) able to communicate with a smart card (31). The transaction terminal includes a processor and memory, and is further able to communicate with another, physically discrete computer (server Sap or electronic unit) that runs a main software application (54/154) for conducting electronic transactions. The main application provides requests for information (signature, authentication, etc.) to the transaction terminal, where filter software F (62) that is installed either on the terminal or on the smartcard operates to translate the high-level requests from the main application into elementary commands that can be executed by the smartcard. The filter software is also adapted to recognize whether the request is legitimate by verifying the identity of the main application from which the requests are received. It is important to note that the only method disclosed by Audebert for this type of verification is by the inclusion in the high-level requests of "information enabling the filter software F to verify its source and its integrity. Authentication can use a Message Authentication Code (MAC) or a code of the electronic signature type associated with the request. If the transaction is not entered by the user on the terminal module itself, the request can contain the information needed for the user to verify the essential data of the transaction, if required and if the terminal module supports this option." [col. 10 ll. 55-59] It is also of note that the filter software F is downloaded from the server Sap, and that the integrity of the filter software is also

verified upon receipt: "To this end a message authentication code (MAC) can be associated with the downloaded program for verifying not only its integrity but also its source. The MAC can be generated using a symmetrical cryptography mechanism (DES in chained CBC mode). The source and integrity can also be verified using an asymmetrical cryptography mechanism: a condensate of the downloaded software is signed by the sender using their private key; the secure microprocessor 3 then verifies the signature using the sender's public key." [col. 23 l. 61 – col. 24 l. 3] Applicants note that all such data verification and authentication by Audebert is thus based upon information contained within the transmitted data itself.

In the Action, the Examiner asserts that "the electronic unit or the server Sap corresponds to the recited computing platform," "the terminal corresponds to the recited monitoring component" and that the smart card corresponds to the recited token device, and proceeds to find that Audebert discloses that said monitoring component is configured to perform a plurality of data checks on said computing platform by reasoning that "the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from said application." Applicants respectfully submit that this interpretation of Audebert is incorrect.

The terminal of Audebert does indeed verify the integrity of data received from the server, but it is of paramount importance to understand that this is **not** the same as performing data checks **on** the server. The terminal of Audebert first receives data from the server and then, once the received data is in its possession, verifies its integrity – in other words, the terminal performs data integrity checks on the terminal, not on the server. This is not a mere matter of semantics; by performing data checks on the computing platform, the claimed invention assures the integrity of the platform itself, whereas the approach of Audebert can do no more than verify the integrity of the received data. Thus, as one illustrative example, the computing platform could be operating under the command of a rogue process that directs it to send data that would be verified as well as authenticated when received by the terminal of Audebert with no possibility of detecting the fact that the platform has been compromised. This is one type

of scenario that the presently claimed invention seeks to subvert by providing a monitoring component that performs data checks on the computing platform.

On a more general level, Applicants note that Audebert is in effect concerned with the integrity of the terminal and with methods of preventing the downloading of malicious code onto, or acceptance of compromised data by, the terminal. Audebert does not in fact address at all the issue of server (computing platform) security. For this reason, Audebert teaches no more than verifying the identity of the server as it is coded into the transmitted data, and does not undertake any actions that can be understood as verifying the integrity of the server.

In view of the above, Applicants respectfully submit that claims 1 and 48 are in fact novel and allowable over Audebert and request the Examiner to kindly reconsider and pass these claims to issue.

Claims 2-16 and 45 depend from claim 1 and claims 49-58 depend from claim 48. In view of the above, Applicants submit that claims 2-16 and 49-58 are also allowable at least based on their dependencies.

With respect to claims 17, 18 and 59, Applicants submit that the above discussion of claims 1 and 48 is equally probative of the novelty of these claims, and thus respectfully request the Examiner to pass these claims to issue as well.

Claims 19-24 and 46 depend from claim 18. Therefore, in light of the above discussion of claim 18, Applicants submit that claims 19-24 and 46 are also allowable, and these claims are not further individually addressed herein.

With regard to claim 25, the Examiner once again finds that Audebert discloses all claimed limitations including, *inter alia*, the claimed receiving an interrogation request signal via an interface of said computing entity and said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal. Applicants once again respectfully disagree. Erstwhile, there is no interrogation request signal received by the server (computing platform) of Audebert; on the contrary, the requests in Audebert flow from the server to

the terminal. There are no requests flowing from the terminal to the server because the terminal verifies the identity of the server solely based on the information contained in the requests received from the server. For this same reason, Audebert does no in fact disclose any actions that can be understood as performing a monitoring operation of the computing platform in response to a received interrogation request signal: namely, because (a) no such interrogation request signal is received by the computing platform, and (b) the only thing monitored by the terminal is the data received **from** the computing platform, not the computing platform itself. Applicants thus respectfully submit that claims 25 is also not anticipated by Audebert and request the Examiner to kindly withdraw this rejection and pas the claim to issue.

Claims 26-31 depend from claim 25. Therefore, in light of the above discussion of claim 25, Applicants submit that claims 26-31 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 32, Applicants make note of the previous discussion respecting claim 25, and in particular that there is no monitoring operation conducted by the terminal of Audebert, and thus there is no possibility of reporting a result message to said token device, said result message describing a result of a monitoring operation, in the system of Audebert. Applicants therefore submit that claim 32 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

Claims 33-37 depend from claim 32. Therefore, in light of the above discussion of claim 32, Applicants submit that claims 33-37 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 38, Applicants again refer to the above discussion and submit that Audebert does not disclose, at the very least, the claimed said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device. As previously shown, Audebert does not teach nor allude to anything akin to performing a verification operation of the computer platform, but rather merely of information received from the computer platform. Applicants thus submit that claim 38 is allowable and respectfully request the Examiner

to reconsider and pass this claim to issue.

With regards to claim 42, Applicants submit that the above discussion clearly proves that Audebert does not in fact disclose the claimed said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity, and said token device receiving a result message describing the result of said verification, because there is no such verification being requested or conducted by or within the system of Audebert. Applicants thus submit that claim 42 is allowable and respectfully request the Examiner to reconsider and pass this claim to issue.

With regards to claim 43, Applicants refer to the above discussion of claims 1 and 48 wherein it was shown that Audebert does not disclose the claimed monitoring component being capable of performing at least one data check on said computer platform. Applicants thus respectfully submit that claim 43 is not in fact anticipated and request the Examiner to reconsider and pass this claim to issue.

With regards to claims 44 and 47, Applicants are in respectful disagreement with the Examiner but, in the interest of passing this case to issue, have cancelled this claim without prejudice and expressly reserving the right to pursue this claim in a related application.

Applicants acknowledge with gratitude the Examiner's indication of allowability as to claim 27 but, as set forth above, Applicants believe that all claims are in fact allowable.

Regarding the prior art made of record by the Examiner but not relied upon, Applicants believe that this art does not render the pending claims unpatentable.

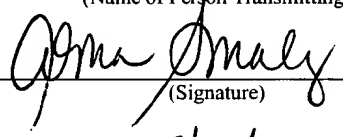
In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

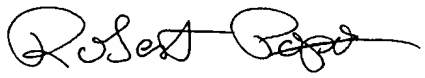
May 24, 2006
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)


(Signature)

5/24/06
(Date)

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com